AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of authenticating a user identity module implemented in an access terminal, comprising:

receiving, at the access terminal and over an air interface, a first Challenge Handshake Authentication Protocol (CHAP) challenge associated with a first authentication process;

deriving, at the access terminal, a second challenge associated with a second authentication process based on at least a portion of the first CHAP challenge;

performing, at the user identity module, the second authentication process using the derived second challenge and producing at least one authentication parameter therefrom; ~~and~~

deriving, at the access terminal, a key associated with the first authentication process based on the at least one authentication parameter; and

re-authenticating the access terminal using the key in response to receiving a second CHAP challenge for re-authentication of the first authentication process.

2. (Canceled)

3. (Currently Amended) A method, as set forth in claim ~~2~~1, wherein deriving the second challenge associated with the second authentication process based on at least a portion of the first challenge further comprises deriving a random number (RAND) challenge based on at least a portion of the first CHAP challenge.

4. (Currently Amended) A method, as set forth in claim 3, wherein deriving the RAND challenge based on at least a portion of the first CHAP challenge further comprises deriving the RAND challenge from a selected number of least significant bits in the first CHAP challenge.

5. (Currently Amended) A method, as set forth in claim 4, wherein performing the second authentication process using the derived second challenge and producing at least one authentication parameter therefrom further comprises performing a cellular authentication and voice encryption (CAVE) based authentication process on the RAND challenge to produce a short message encryption key (SMEKEY).

6. (Currently Amended) A method, as set forth in claim 5 wherein performing the CAVE based authentication process on the RAND challenge to produce SMEKEY further comprises performing the CAVE based authentication process on the RAND challenge to produce the SMEKEY and a public long code mask (PLCM).

7. (Original) A method, as set forth in claim 6, wherein deriving the key associated with the first authentication process based on the at least one authentication parameter further comprises deriving the key associated with the first authentication process based on SMEKEY and PLCM.

8. (Currently Amended) A method, as set forth in claim 1, further comprising:

generating, at the access terminal, an authentication response to the first CHAP challenge based on the key; and

delivering the authentication response over the air interface to a network to request access to the network.

9. (Currently Amended) A method, as set forth in claim 8, ~~further comprising~~ wherein re-authenticating the access terminal comprises:

determining that the ~~first~~ second CHAP challenge associated with the first authentication process is a re-authentication challenge;

bypassing the derivation of the second challenge associated with the second authentication process based on at least a portion of the ~~first~~ second CHAP challenge in response to the determining that the second CHAP ~~first~~ challenge is the re-authentication challenge;

bypassing the performance of the second authentication process using the derived second challenge and producing at least one authentication parameter therefrom in response to the determining that the second CHAP ~~first~~ challenge is the re-authentication challenge; and wherein

deriving the key associated with the first authentication process based on the at least one authentication parameter further comprises using a previously derived key in response to the determining that the second CHAP ~~first~~ challenge is the re-authentication challenge.

10. (Currently Amended) A method, as set forth in claim ~~8~~9, further comprising:

determining that the second CHAP ~~first~~ challenge associated with the first authentication process is a re-authentication challenge; and wherein

delivering the key to a network to request access to the network further comprises delivering ~~a~~ the previously derived key in response to the determining that the second CHAP ~~first~~ challenge is the re-authentication challenge.

11. (Currently Amended) A method, comprising:

~~receiving~~ determining, at an access terminal, whether a CHAP challenge is an authentication challenge or a re-authentication challenge;

~~deriving a RAND challenge based on at least a portion of the CHAP challenge;~~

~~performing an authentication using the RAND challenge to produce a SMEKEY and a PLCM; and~~

~~deriving~~ providing, from the access terminal, a response formed from a secret CHAP key derived using information retrieved from a subscriber identity module in the access terminal when the CHAP challenge is an authentication challenge ~~based on the SMEKEY and PLCM~~; and

providing, from the access terminal, a response formed from a previously derived secret CHAP key when the CHAP challenge is a re-authentication challenge.